Calendar No. 563

104TH CONGRESS, 2d Session | SENATE | REPORT 104–357

THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995

AUGUST 27, 1996.—Ordered to be printed

Filed under the authority of the order of the Senate of August 2, 1996

Mr. HATCH, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 982]

The Committee on the Judiciary, to which was referred the bill (S. 982) to amend the Computer Fraud and Abuse Act, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Information Infrastructure Protection Act of 1996".

SEC. 2. COMPUTER CRIME.

Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking "knowingly accesses" and inserting "having knowingly accessed";

(ii) by striking "exceeds" and inserting "exceeding";

(iii) by striking "obtains information" and inserting "having obtained information";

(iv) by striking "the intent or";

(v) by striking "is to be used" and inserting "could be used"; and

(vi) by inserting before the semicolon at the end the following: "willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it";

(B) in paragraph (2)—

(i) by striking "obtains information" and inserting "obtains—

"(A) information"; and

(ii) by adding at the end the following new subparagraph:

"(B) information from any department or agency of the United States; or

"(C) information from any protected computer if the conduct involved an interstate or foreign communication;";

(C) in paragraph (3)—

(i) by inserting "nonpublic" before "computer of a department or agency";

(ii) by striking "adversely"; and

(iii) by striking "the use of the Government's operation of such computer" and inserting "that use by or for the Government of the United States";

(D) in paragraph (4)—

(i) by striking "Federal interest" and inserting "protected"; and

(ii) by inserting before the semicolon the following: "and the value of such use is not more than $5,000 in any 1-year period";

(E) by striking paragraph (5) and inserting the following:

"(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

"(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

"(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;"; and

(F) by inserting after paragraph (6) the following new paragraph:

"(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;";

(2) in subsection (c)—

(A) in paragraph (1), by striking "such subsection" each place that term appears and inserting "this section";

(B) in paragraph (2)—

(i) in subparagraph (A)—

(I) by inserting ", (a)(5)(C)," after "(a)(3)"; and

(II) by striking "such subsection" and inserting "this section";

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting immediately after subparagraph (A) the following:

"(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if—

"(i) the offense was committed for purposes of commercial advantage or private financial gain;

"(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

"(iii) the value of the information obtained exceeds $5,000;"; and

(iv) in subparagraph (C) (as redesignated),

(i) by striking "such subsection" and inserting "this section"; and

(II) by adding "and" at the end;

(C) in paragraph (3)—

(i) in subparagraph (A)—

(I) by striking "(a)(4) or (a)(5)(A)" and inserting "(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)"; and

(II) by striking "such subsection" and inserting "this section"; and

(ii) in subparagraph (B)—

(I) by striking "(a)(4) or (a)(5)" and inserting "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)"; and

(II) by striking "such subsection" and inserting "this section"; and

(D) by striking paragraph (4);

(3) in subsection (d), by inserting "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of" before "this section.";

(4) in subsection (e)—

(A) in paragraph (2)—

(i) by striking "Federal interest" and inserting "protected";

(ii) in subparagraph (A), by striking "the use of the financial institution's operation or the Government's operation of such computer" and inserting "that use by or for the financial institution or the Government"; and

(iii) by striking subparagraph (B) and inserting the following:

"(B) which is used in interstate or foreign commerce or communication;";

(B) in paragraph (6), by striking "and" at the end;

(C) in paragraph (7), by striking the period at the end and inserting "; and"; and

(D) by adding at the end the following new paragraphs:

"(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that—

"(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

"(C) causes physical injury to any person; or

"(D) threatens public health or safety; and

"(9) the term 'government entity' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country."; and

(5) in subsection (g)—

(A) by striking ", other than a violation of subsection (a)(5)(B),"; and

(B) by striking "of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)" and inserting "involving damage as defined in subsection (e)(8)(A)".

I. PURPOSE

The Leahy-Kyl-Grassley amendment to the National Information Infrastructure (NII) Protection Act, S. 982, would strengthen the Computer Fraud and Abuse Act, 18 U.S.C. 1030, by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks.

II. LEGISLATIVE HISTORY

The Computer Fraud and Abuse Act was originally enacted in 1984 to provide a clear statement of proscribed activity concerning computers to the law enforcement community, those who own and operate computers and those tempted to commit crimes by unauthorized access to computers. Rather than having to "boot-strap" enforcement efforts against computer crime by relying on statutory restrictions designed for other offenses, the Computer Fraud and Abuse statute, 18 U.S.C. 1030, set forth in a single statute computer-related offenses. This first Federal computer crime statute made it a felony to access classified information in a computer without authorization and a misdemeanor to access financial

records or credit histories in financial institutions or to trespass into a Government computer.

In succeeding years, the statute has been significantly amended only twice, in 1986 and 1994. In its current form, this statute generally prohibits the unauthorized use of computers to obtain classified or private financial record information, to trespass in Federal Government computers, to commit frauds, or to transmit harmful computer viruses. It also prohibits fraudulent trafficking in computer access passwords.

Gaps in coverage remain under this statutory scheme. Specifically, the law provides criminal penalties for persons who, without or in excess of authorization, access any computer to obtain classified information or financial record information from a financial institution or consumer reporting agency, or who access a "Federal interest computer" to further an intended fraud. A "Federal interest computer" is defined to include Federal Government and financial institution computers and computers located in different States that are "used in committing the offense."

The privacy protection coverage of the statute has two significant gaps. First, omitted from the statute's coverage is information on any civilian or State and local government computers, since the prohibition on unauthorized computer access to obtain nonclassified information extends only to computers used by financial institutions or by the Federal Government when the perpetrator is an outsider. The second gap is the significant limitation on the privacy protection given to information held on Federal Government computers. Specifically, the prohibition only applies to outsiders who gain unauthorized access to Federal Government computers, and not to Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential.

Likewise, omitted from the fraud protection coverage of the statute is protection for the loss of computer time resulting from computer trespasses. The 1986 amendments to the statute created the "computer use" exception to section 1030(a)(4), even though this Committee "agree[d] that lost computer time resulting form repeated or sustained trespasses can reach a level of seriousness sufficient to warrant Federal prosecution." Senate Judiciary Committee report No. 99–432, 99th Cong., 2d sess., at p. 10 (1986). At the time of the 1986 amendments, such fraudulent computer usage was considered prosecutable under another section 1030(a)(5), when the lost computer time resulted from intentional damage to the computer.

The current statute also penalizes any person who uses a computer in interstate commerce or communications to cause the transmission of a computer virus or other harmful computer program. Omitted from the coverage of this "computer damage" provision are Government and financial institution computers not used in interstate communications, such as intrastate local area networks used by Government agencies that contain sensitive and confidential information. Also omitted are computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based. For example, the 1994 intrusion into the Rome Laboratory at Grifess Air Force Base in New York, was perpetrated

by a 16-year-old hacker in the United Kingdom. More recently, in March 1996, the Justice Department tracked down a young Argentinean man who had broken into Harvard University's computers from Buenos Aires and used those computers as a staging ground to hack into many other computer sites, including the Defense Department and NASA.

On June 29, 1995, Senators Kyl, Leahy, and Grassley introduced the NII Protection Act, S. 982. At hearings in both the House of Representatives and the Senate, representatives from Federal law enforcement agencies expressed the need for, and their support of, this bill. Specifically, Attorney General Janet Reno discussed the provisions of S. 982 in her October 30, 1995, responses to written questions in connection with the June 27, 1995, Judiciary Committee oversight hearing of the Department of Justice; Federal Bureau of Investigation Director Louis Freeh testified about S. 982 during the February 28, 1996, joint hearing with the Select Committee on Intelligence and the Judiciary Committee on economic espionage; and U.S. Secret Service Deputy Assistant Director of Investigations Robert Rasor testified about S. 982 during the October 11, 1995, hearing of the House Committee on Banking and Financial Services Subcommittee on Domestic and International Monetary Policy.

As intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology. As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime. The NII Protection Act will likely not represent the last amendment to this statute, but is necessary and constructive legislation to deal with the current increase in computer crime.

III. COMMITTEE ACTION

On June 13, 1996, the Committee on the Judiciary first considered the NII Protection Act, S. 982, as an amendment made by Senators Leahy, Kyl, and Grassley to H.R. 1533, a bill to amend title 18, United States Code, to increase the penalty for escaping from a Federal prison. At that time, with a quorum present, by voice vote, the Committee unanimously accepted the Leahy-Kyl-Grassley amendment to H.R. 1533, and unanimously ordered H.R. 1533, so amended, favorably reported.

On August 1, 1996, the Committee on the Judiciary, with a quorum present, again accepted an amendment in the nature of a substitute to S. 982 offered by Senator Leahy, on behalf of himself and Senators Kyl and Grassley. The amendment included the provisions in the S. 982, as introduced, with one modification. As discussed in more detail below, the amendment inserted the word "nonpublic" before "computer of a department or agency" in section 2(1)(C)(I) of the bill. The Leahy-Kyl-Grassley amendment was accepted by voice vote, and the Committee, also by voice vote, then unanimously ordered S. 982, as amended, favorably reported.

IV. SECTION-BY-SECTION ANALYSIS

DETAILED DISCUSSION OF THE NII PROTECTION ACT

The bill amends five of the prohibited acts in, and adds a new prohibited act to, 18 U.S.C. 1030(a). Each of the amended provisions is discussed below.

(1) Amendments and addition to prohibited acts

(A) Subsection 1030(a)(1)—Protection of classified government information

The bill would bring the protection for classified national defense or foreign relations information maintained on computers in line with our other espionage laws. Section 1030(a)(1) currently provides that anyone who knowingly accesses a computer without authorization or exceeds authorized access and obtains classified information "with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation" is subject to a fine or imprisonment for not more than 10 years for a first offense. This scienter element apparently was originally included because it is contained in 18 U.S.C. 794(a). Section 794(a), however, provides for life imprisonment, whereas section 1030(a)(1) provides for only a 10-year term of imprisonment. Therefore, the NII Protection Act would amend section 1030(a)(1) to track the scienter requirement of 18 U.S.C. 793(e), which also provides a maximum penalty of 10 years imprisonment for obtaining from any source certain items relating to the national defense.

As amended, section 1030(a)(1) prohibits anyone from knowingly accessing a computer, without, or in excess of, authorization, and obtaining classified national defense, foreign relations information, or restricted data under the Atomic Energy Act, with reason to believe the information could be used to the injury of the United States or the advantage of a foreign country, and willfully communicating, delivering or transmitting, or causing the same, or willfully retaining the information and failing to deliver it to the appropriate Government agent. The amendment specifically covers the conduct of a person who deliberately breaks into a computer without authority, or an insider who exceeds authorized access, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities.

Although there is considerable overlap between 18 U.S.C. 793(e) and section 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately break into a computer to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, section 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this sense then, it is the use of the computer which is being proscribed, not the un-

authorized possession of, access to, or control over the classified information itself.

(B) Subsection 1030(a)(2)—Protection of financial, Government and other computer information

The bill would amend section 1030(a)(2) to increase protection for the privacy and confidentiality of computer information. Section 1030(a)(2) currently gives special protection only to information on the computer systems of financial institutions and consumer reporting agencies, because of their significance to our country's economy and the privacy of our citizens. Yet, increasingly computer systems provide the vital backbone to many other industries, such as transportation, power supply systems, and telecommunications. The bill would amend section 1030(a)(2) and extend its coverage to information held on (1) Federal Government computers and (2) computers used in interstate or foreign commerce on communications, if the conduct involved an interstate or foreign communication.

As amended, section 1030(a)(2) would penalize those who intentionally access computers without, or in excess of, authorization to obtain government information and, where appropriate, information held on private computers.

"Information" as used in this subsection includes information stored in intangible form. Moreover, the term "obtaining information" includes merely reading it. There is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be "stolen" without asportation, and the original usually remains intact. This interpretation of "obtaining information" is consistent with congressional intent expressed as follows in connection with 1986 amendments to the Computer Fraud and Abuse statute:

> Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the date from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.

Senate Judiciary Committee report No. 99–432, 99th Cong., 2d sess., at pp. 6–7 (1986).

The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. This information, stored electronically, is intangible, and it has been held that the theft of such information cannot be charged under more traditional criminal statutes such as Interstate Transportation of Stolen Property, 18 U.S.C. 2314. See *United States* v. *Brown,* 925 F.2d 1301, 1308 (10th Cir. 1991). This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection

1030(a)(2)(C), however, is the abuse of a computer to obtain the information.

The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or on what is planned for the information after it is obtained. Thus, the statutory penalties are structured to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways, is a felony.

The sentencing scheme for section 1030(a)(2) is part of a broader effort to ensure that sentences for section 1030 violations adequately reflect the nature of the offense. Thus, under the bill, the harshest penalties are reserved for those who obtain classified information that could be used to injure the United States or assist a foreign state. Those who improperly use computers to obtain other types of information—such as financial records, nonclassified Government information, and information of nominal value from private individuals or companies—face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortious act.

For example, individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000.

The terms "for purposes of commercial advantage or private financial gain" and "for the purpose of committing any criminal or tortious act" are taken from the copyright statute (17 U.S.C. 506(a)) and the wiretap statute (18 U.S.C. 2511(1)(d)), respectively, and are intended to have the same meaning as in those statutes.

Some conduct may violate more than one subsection of section 1030(a)(2). For example, a particular Government computer might be covered by both sections 1030(a)(2)(B) and (a)(2)(C). This overlap serves to eliminate legal issues that may arise if the provisions were mutually exclusive. Conceivably, in a given case, it may not be clear whether information taken from a Government contractor's computer constitutes "information from any department or agency of the United States" under section 1030(a)(2)(B), but the offense might still be chargeable under section 1030(a)(2)(C) if the elements of that subsection are satisfied. Similarly, there may be some overlap between section 1030(a)(2) and 18 U.S.C. 641 (relating to the theft and conversion of public money, records or property), but the former does not preempt the latter.

(C) Subsection 1030(a)(3)—Protection for Government computer systems

The NII Protection Act would make three modifications to subsection 1030(a)(3), which is focused on providing protection to Federal Government computers from outside hackers. This provision currently prohibits a person from intentionally accessing, without

authorization, a Federal Government computer and, if the computer is not exclusively used by the Government, then the conduct must "adversely affect[] the use of the Government's operation of such computer."

First, the bill would delete the word "adversely" because this term suggests, inappropriately, that trespassing in a computer used by the Federal Government, even if not exclusively, may be benign. Second, the bill would modify "computer of a department or agency of the United States" with the term "non-public." This would make clear that unauthorized access is barred to any "nonpublic" Federal Government computer and that a person who is permitted to access publicly available Government computers, for example, via an agency's World Wide Web site, may still be convicted under (a)(3) for accessing without authority any nonpublic Federal Government computer. Finally, the phrase "the use of the Government's operation of such computer" would be clarified with the term "that use." When a computer is used for the Government, the Government is not necessarily the operator, and the old phrase may lead to confusion. Consistent with this change, a similar change is made by the NII Protection Act in the reference to government and financial institution computers in the new definition of "protected computer" in section 1030(e)(2)(A).

(D) Subsection 1030(a)(4)—Increased penalties for significant unauthorized use of computers

The bill amends 18 U.S.C. 1030(a)(4) to ensure that sanctions apply when the fraudulent use of a computer without, or in excess of, authority is significant. The current statute penalizes, with fines and up to 5 years' imprisonment, knowingly accessing a computer with the intent to defraud and by means of such conduct furthering the fraud and obtaining anything of value. This provision contains a "computer use" exception that exempts fraudulent conduct to obtain only the use of the computer. While every trespass in a computer should not be converted into a felony scheme to defraud, a blanket exception for "computer use" is too broad. Hackers, for example, have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far more than $5,000. In light of the large expense to the victim caused by some of these trespassing incidents, the amendment would limit the "computer use" exception to cases where the stolen computer use involved less than $5,000 during any one-year period.

(E) Subsection 1030(a)(5)—Protection from damage to computers

The bill amends subsection 1030 (a)(5) to further protect computers and computer systems covered by the statute from damage both by outsiders, who gain access to a computer without authorization, and by insiders, who intentionally damage a computer. The law currently protects computers or computer systems from damage caused by either outside hackers or malicious insiders "through means of a computer used in interstate commerce or communications."

Senator Leahy was the principal sponsor of the 1994 amendment to subsection 1030(a)(5), which was intended to broaden the reach of the provision by replacing the term "federal interest computer" with the term "computer used in interstate commerce or communication." The latter term is broader because the definition of "federal interest computer" in section 1030(e)(2)(B) covers a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State." This meant that hackers who attacked other computers in their own State were not subject to Federal jurisdiction, notwithstanding the fact that their actions may have severely affected interstate or foreign commerce. For example, individuals who attack telephone switches may disrupt interstate and foreign calls. The 1994 change remedied that defect.

The definition of Federal interest computer, however, actually covered more than simply interstate activity. More specifically, section 1030(e)(2)(A) covered, generically, computers belonging to the U.S. Government or financial institutions, or those used by such entities on a nonexclusive basis if the conduct constituting the offense affected the Government's operation or the financial institution's operation of such computer. By changing section 1030(a)(5) from "federal interest computer" to "computer used in interstate commerce or communication" in the 1994 amendment, Congress inadvertently eliminated Federal protection for those Government and financial institution computers not used in interstate communications. For example, the integrity and availability of classified information contained in an intrastate local area network may not have been protected under the 1994 version of section 1030(a)(5), although its confidentiality continued to be protected under section 1030(a)(1).

Thus, the current provision falls short of protecting government and financial institution computers from intrusive codes, such as computer "viruses" or "worms." Generally, hacker intrusions that inject "worms" or "viruses" into a government or financial institution computer system which is not used in interstate communications is not a Federal offense. The NII Protection Act would change that limitation and extend Federal protection from intentionally damaging viruses to government and financial institution computers, even if they are not used in interstate communications.

Specifically, as amended, subsection 1030(a)(5)(A) would penalize, with a fine and up to 5 years' imprisonment, anyone who knowingly causes the transmission of a program, information, code or command and intentionally causes damage to a protected computer. This would cover anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer. Subsection 1030(a)(5)(B) would penalize, with a fine and up to 5 years' imprisonment, anyone who intentionally accesses a protected computer without authorization and, as a result of that trespass, recklessly causes damage. This would cover outsiders hackers into a computer who recklessly cause damage. Finally, subsection 1030(a)(5)(C) would impose a misdemeanor penalty, of a fine and up to 1 year imprisonment, for intentionally accessing a protected computer without authorization and, as a result of that trespass, causing

damage. This would cover outside hackers into a computer who negligently or accidentally cause damage.

In sum, under the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.

The rationale for this difference in treatment deserves explanation. Although those who intentionally damage a system, without authority, should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, it is no crime unless that damage was either intentional or reckless. Rather than send such a dangerous message (and deny victims any relief), it is better to ensure that section 1030(a)(5) criminalizes all computer trespass, as well as intentional damage by insiders, albeit at different levels of severity.

The 1994 amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no "damage," the victim does suffer "loss." If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

The bill therefore defines "damage" in new subsection 1030(e)(8), with a focus on the harm that the law seeks to prevent. As in the past, the term "damage" will require either significant financial losses under section 1030(e)(8)(A), or potential impact on medical treatment under section 1030(e)(8)(B). The bill addresses two other concerns: causing physical injury to any person under new section 1030(e)(8)(C), and threatening the public health or safety under new section 1030(e)(8)(D). As the NII and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate. Thus, the definition of "damage" is amended to be sufficiently broad to encompass the types of harm against which people should be protected.

The bill also amends the civil penalty provision under section 1030(g) to be consistent with the amendments to section 1030(a)(5). The amendment to section 1030(g) provides that victims of com-

puter abuse can maintain a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief. Damages are limited to economic damages, unless the defendant violated section 1030(a)(5)(A) or section 1030(a)(5)(B); that is, unless the actor intentionally caused damage, or recklessly caused damage while trespassing in a computer.

(F) Subsection 1030(a)(7)—Protection from threats directed against computers

The bill would add a new subsection (a)(7) to section 1030 to address a new and emerging problem of computer-age blackmail. This is a high-tech variation on old fashioned extortion. According to the Department of Justice, threats have been made against computer systems in several instances. One can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key. This new provision would ensure law enforcement's ability to prosecute modern-day blackmailers, who threaten to harm or shut down computer networks unless their extortion demands are met.

The Attorney General explained in written responses to questions of Senator Leahy on October 30, 1995:

> These cases, although similar in some ways to other cases involving extortionate threats directed against persons or property, can be different from traditional extortion cases in certain respects. It is not entirely clear that existing extortion statutes, which protect against physical injury to person or property, will cover intangible computerized information.

For example, the "property" protected under existing laws, such as the Hobbs Act, 18 U.S.C. 1951 (interference with commerce by extortion), or 18 U.S.C. 875(d) (interstate communication of threat to injure the property of another), does not clearly include the operation of a computer, the data or programs stored in a computer or its peripheral equipment, or the decoding keys to encrypted data.

New section 1030(a)(7) would close this gap in the law and provide penalties for the interstate or international transmission of threats directed against computers and computer systems. This covers any interstate or international transmission of threats against computers, computer networks, and their data and programs whether the threat is received by mail, a telephone call, electronic mail, or through a computerized messaging service. Unlawful threats could include interference in any way with the normal operation of the computer or system in question, such as denying access to authorized users, erasing or corrupting data or programs, slowing down the operation of the computer or system, or encrypting data and then demanding money for the key.

(2) Subsection 1030(c)—Increased penalties for recidivists and other sentencing changes

The bill amends 18 U.S.C. 1030(c) to increase penalties for those who have previously violated any subsection of section 1030(a). The current statute subjects recidivists to enhanced penalties only if they violated the same subsection twice. For example, a person who

violates the current statute by committing fraud by computer under subsection 1030(a)(4) and later commits another computer crime offense by intentionally destroying medical records under subsection 1030(a)(5), is not treated as a recidivist because his conduct violated two separate subsections of section 1030. The amendment provides that anyone who is convicted twice of committing a computer offense under subsection 1030(a) would be subjected to enhanced penalties.

The penalty provisions in section 1030(c) are also changed to reflect modifications to the prohibited acts, as discussed above.

(3) Subsection 1030(d)—Jurisdiction of Secret Service

The bill amends subsection 1030(d) to grant the U.S. Secret Service authority to investigate offenses only under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The current statute grants the Secret Service authority to investigate any offense under section 1030, subject to agreement between the Attorney General and the Secretary of the Treasury. The new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

(4) Subsection 1030(e)—New definitions

The NII Protection Act strikes the current definition of "Federal interest computer" and adds new definitions for "protected computer," "damage," and "government entity."

The bill would amend subsection 1030(e)(2) by replacing the term "Federal interest computer" with the new term "protected computer" and a new definition. The new definition of "protected computer" would modify the current description in subsection 1030(e)(2)(A) of computers used by financial institutions or the U.S. Government, to make clear that if the computers are not exclusively used by those entities, the computers are protected if the offending conduct affects the use by or for a financial institution or the Government. The new definition also replaces the current limitation in subsection 1030(e)(2)(B) of "Federal interest computer" being "one of two or more computers used in committing the offense, not all of which are located in the same State." Instead, "protected computer" would include computers "used in interstate or foreign commerce or communications." Thus, hackers who steal information or computer usage from computers in their own State would be subject to this law, under amended section 1030(a)(4), if the requisite damage threshold is met and the computer is used in interstate commerce or foreign commerce or communications.

The term "damage" in new subsection 1030(e)(8), as used in the proposed amendment of subsection 1030(a)(5), would mean any impairment to the integrity or availability of data, information, program or system which (A) causes loss of more than $5,000 during any 1-year period; (B) modifies or impairs the medical examination,

diagnosis or treatment of a person; (C) causes physical injury to any person; or (D) threatens the public health or safety.

The term "government entity" in new subsection 1030(e)(9), as used in the new proposed subsection 1030(a)(7), would be defined to include the U.S. Government, any State or political subdivision thereof, any foreign country, and any state, provincial, municipal, or other political subdivision of a foreign country.

(5) Subsection 1030(g)—Civil actions

The bill amends the civil penalty provision in subsection 1030(g) to reflect the proposed changes in subsection 1030(a)(5). The 1994 amendments to the act authorized certain victims of computer abuse to maintain civil actions against violators to obtain compensatory damages, injunctive relief, or other equitable relief, with damages limited to economic damages, unless the violator modified or impaired the medical examination, diagnosis or treatment of a person.

Under the bill, damages recoverable in civil actions by victims of computer abuse would be limited to economic losses for violations causing losses of $5,000 or more during any 1-year period. No limit on damages would be imposed for violations that modified or impaired the medical examination, diagnosis or treatment of a person; caused physical injury to any person; or threatened the public health or safety.

V. Regulatory Impact Statement

Pursuant to paragraph 11(b), rule XXVI of the Standing Rules of the Senate, the Committee, after due consideration, concludes that Senate bill 982 will not have direct regulatory impact.

VI. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, August 6, 1996.

Hon. Orin G. Hatch,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 982, the National Information Infrastructure Protection Act of 1996, as reported by the Senate Committee on the Judiciary on August 2, 1996.

Enacting S. 982 could affect direct spending and receipts. Therefore, pay-as-you-go procedures would apply to this bill.

If you wish further details on this estimate, we will be pleased to provide them.

Sincerely,

James L. Blum
(For June E. O'Neill).

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

1. Bill number: S. 982.

2. Bill title: National Information Infrastructure Protection Act of 1996.

3. Bill status: As reported by the Senate Committee on the Judiciary on August 2, 1996.

4. Bill purpose: S. 982 would make various amendments to the laws that protect the confidentiality, integrity, and security of computer systems and the information maintained on such systems. In particular, the bill would amend existing statutes relating to five computer-related crimes and would add a new statute making the interstate transmission of threats directed against computers or computer systems a federal crime.

5. Estimated cost to the Federal Government: CBO estimates that enacting S. 982 would not have any significant budgetary impact. Although the legislation could affect direct spending and receipts, we estimate that any such changes would be negligible.

6. Basis of estimate: Based on information from the U.S. Sentencing Commission, CBO expects that enacting S. 982 could increase the number of prosecutions brought by the federal government and could increase governmental receipts from penalties for committing computer-related crimes. Fewer than 50 persons are convicted of existing computer-related crimes each year and CBO does not expect that the caseload under S. 982 would increase significantly. Thus, CBO estimates that the Justice Department would not need significant additional resources to enforce the provisions of the bill.

Furthermore, CBO estimates that any increase in prison time served by people prosecuted under the statutes affected by S. 982 would be negligible and that the government would collect less than $500,000 a year in additional fines. Such fines are recorded in the budget as governmental receipts, deposited in the Crime Victims Fund, and spent in the following year. Because the increase in direct spending would be the same as the amount of fines collected with a one-year lag, the additional direct spending also would be less than $500,000 a year.

7. Pay-as-you-go considerations: Section 252 of the Balanced Budget and Emergency Deficit Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts through 1998. S. 982 would establish new fines and increase some existing ones. CBO expects that any additional receipts would be negligible and thus the pay-as-you-go impact of this bill, as shown in the following table, also would be negligible.

[By fiscal year, in millions of dollars]

	1996	1997	1998
Change in outlays	0	0	0
Change in receipts	0	0	0

8. Estimated impact on State, local, and tribal governments: S. 982 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act of 1995 (Public Law 104–4) and would not impose costs on State, local, or tribal governments.

9. Estimated impact on the private sector: This bill would impose no new private-sector mandates as defined in Public Law 104–4.

10. Previous CBO estimate: On July 25, 1996, CBO transmitted a cost estimate for H.R. 1533, the Sexual Offender Tracking and Identification Act of 1996, as reported by the Senate Committee on the Judiciary on June 13, 1996. Section 13 of H.R. 1533 is identical to S. 982. The other provisions of H.R. 1533, as approved by the Senate Committee on the Judiciary, were not included in S. 982.

11. Estimate prepared by: Federal cost estimate: Susanne S. Mehlman and Stephanie Weiner. Impact on State, local, and tribal governments: Leo Lex. Impact on the private sector: Matthew Eyles.

12. Estimate approved by: Robert A. Sunshine (for Paul N. Van de Water, Assistant Director for Budget Analysis).

VII. CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the changes in existing law made by the bill, as reported by the committee, are shown as follows (existing law proposed to be omitted is enclosed in bold brackets, new matter is printed in italic, and existing law with no changes is printed in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) **[**knowingly accesses**]** *having knowingly accessed* a computer without authorization or **[**exceeds**]** *exceeding* authorized access, and by means of such conduct **[**obtains information**]** *having obtained information* that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with **[**the intent or**]** reason to believe that such information so obtained **[**is to be used**]** *could be used* to the injury of the United States, or to the advantage of any foreign nation *willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails*

to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby [obtains information] *obtains—*

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any *nonpublic* computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct [adversely] affects [the use of the Government's operation of such computer] *that use by or for the Government of the United States;*

(4) knowingly and with intent to defraud, accesses a [Federal interest] *protected* computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer *and the value of such use is not more than $5,000 in any 1-year period;*

[(5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if

[(i) the person causing the transmission intends that such transmission will

[(I) damage, or causes damage to, a computer, computer system, network, information, data, or program; or

[(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and

[(ii) the transmission of the harmful component of the program, information, code, or command—

[(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

[(II)(aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period; or

[(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis,

medical treatment, or medical care of one or more individuals; or

[(B) through means of a computer used in interstate commerce or communication, and knowingly causes the transmission of a program, information, code, or command to a computer or computer system—

[(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will—

[(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

[(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program; and

[(ii) if the transmission of the harmful component of the program, information, code, or command—

[(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

[(II)(aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1-year period; or

[(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals;]

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; *or*

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under [such subsection] *this section,* or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under [such subsection] *this section,* or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3)*, (a)(5)(C),* or (a)(6) of this section which does not occur after a conviction for another offense under [such subsection] *this section,* or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(2) if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

[B] *(C)* a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under [such subsection] *this section*, or an attempt to commit an offense punishable under this subparagraph; *and*

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection [(a)(4) or (a)(5)(A)] *(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)* of this section which does not occur after a conviction for another offense under [such subsection] *this section,* or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection [(a)(4) or (a)(5)] *(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)* of this section which occurs after a conviction for another offense under [such subsection] *this section,* or an attempt to commit an offense punishable under this subparagraph; and [(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).]

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under *subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of* this section. Such authority of the United

States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term [Federal interest] *protected* computer means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects [the use of the financial institution's operation or the Government's operation of such computer] *that use by or for the financial institution or the Government*; or

[(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State]

(B) which is used in interstate or foreign commerce or communication;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter; [and]

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5[.]; *and*

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information that—

(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) any person who suffers damage or loss by reason of a violation of the section [,other than a violation of subsection (a)(5)(B),] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations [of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)] *involving damage under subsection (e)(8)(A)* are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under section 1030(a)(5) of title 18, United States Code.

○